[0035] § 3. Embodiment showing concrete use mode

Subsequently, a concrete use mode of the above-described IC card will be described following transition of recording contents of a channel setting region shown in FIG. 7. In this embodiment, at a reset time immediately after connecting an IC card 10 to a reader/writer device 20, the recording contents of a channel setting region in a RAM 14 are brought into an initial state as shown in FIG. 8. That is, 2-byte data "FFFF" indicating that identification information is not recorded is written in each recording portion upper stage, and 1-bit data "00000000" indicating that all eight keys are unlocked is written in each recording portion lower stage. It is to be noted that in the following description, for convenience, nine recording portions will be referred to as recording portion (1, 1), recording portion (1, 2), ..., recording portion (3, 3).

[0036] <3-1: Selection No.1 of File Management Region>

In the present invention, an operation of designating a specific channel to select a specific file management region is required as a preparation stage for access to each file. To perform this operation, a selection command having a predetermined format may be given to the IC card 10 from the reader/writer device 20. Here, for example, as shown in FIG. 9①, a case where the selection command is given in format "SELECT #1 DF1" is considered. This selection command is a command for designating a specific channel #1 to select a specific file

management region DF1. When this command is given, a CPU 12 writes identification information of the selected file management region DF1 and a file management region MF disposed in an upper class of the selected region into the upper stage of the recording portion corresponding to each class in the designated channel setting region (channel #1) to obtain a recorded state, and writes unlock information indicating that all the keys are not unlocked into the lower stage of each recording portion. FIG. 9 shows a state of the channel setting region immediately after this process is performed. In actual, 2-byte identification information indicating a specific file management region is written in the upper stage of each recording portion. In the drawing, for the convenience, a state in which each file management region name (MF, DF1) is directly written is shown. To avoid complication in the drawing, an unrecorded state recording portion which is not directly associated with description is shown as a blank column. However, in actual, as shown in FIG. 8, data "FFFF (upper stage)" or "00000000 (lower stage)" is written in the blank column.

[0037] Eventually, in the recording portion constituting each channel setting region, a recording portion including the upper stage which is "FFFF" indicates a recording portion in a unrecorded state, and a recording portion including an upper stage other than "FFFF" indicates a recording portion having a recorded state. Moreover, in

each channel setting region, a file management region in which the identification information is recorded in the recording portion of a lowermost layer in the recorded state is a file management region presently selected with respect to the channel. In an example shown in FIG. 9, the identification information indicating the file management region DF1 is written in the recording portion (2, 1) of the lowermost layer in the recorded state in the region of the channel #1, and therefore the file management region presently selected with respect to the channel #1 is DF1. At this time, the identification information of the file management region MF is written in the recording portion (1, 1) of the upper class of the channel #1. This performs a function of indicating that a parent of the presently selected file management region DF1 in a class structure is MF. Moreover, as described later, setting that the unlock information of the upper class be referred to is possible.

[0038] In the present invention, when the command of designating the specific channel to select the specific file management region is given in this manner, the identification information of the selected file management region and the file management region of the upper class above the shape region is written into the recording portion corresponding to each class in the designated channel setting region, and the recording portion corresponding to the lower class below the selected file management region has an unrecorded state. Therefore, for

example, instead of a selection command "SELECT #1 DF1" shown in FIG. 9①, a selection command "SELECT #1 DF1-2" shown in FIG. 10① is given, and a file management region DF1-2 of class 3 is selected. In this case, recording contents of channel #1 are as shown in FIG. 10. In FIG. 10, since the identification information indicating the file management region DF1-2 is written in the recording portion (3, 1) of the lowermost layer in the recorded state, the file management region presently selected with respect to the channel #1 is DF1-2.

[0039] <3-2: Key Collating No. 1> Subsequently, an update process of the channel setting region in a case where key is collated will be described. In the present invention, the key is collated, when a command for designating the specific channel to perform predetermined key collation is given. For example, as shown in FIG. 9, it is now assumed that the key collation is performed with respect to the selected file management region DF1 in a state in which the file management region DF1 is selected as the channel #1. Here, it is assumed that key K3 is collated with key K5. In this case, first, a collation command "VERIFY #1 K3 ????" may be given as shown in FIG. 11①. Here, "????" is a concrete key security code. The CPU 12 reads the security code of the key K3 from a predetermined key file in the file management region DF1 selected as the channel #1, and compares/collates this code with the key security code "????" given from the outside. Moreover, when both

the codes agree with each other, a process of writing bit "1" indicating an unlocked state in a third bit of the lower stage of the recording portion (2, 1) of FIG. 11 is performed. Subsequently, when a collation command "VERIFY #1K5 ????" is given as shown in FIG. 11②, the key K5 is collated. When the key agrees with the code, a process of writing bit "1" in a fifth bit is performed. A bit state of the recording portion (2, 1) shown in FIG. 11 shows a state immediately after this process is performed.

[0040] Eventually, in the present invention, when the command for designating the specific channel to perform predetermined key collation is given, an update process is performed to update the unlock information recorded in the recording portion (recording portion (2, 1) in the above-described example) of the lowermost layer in the recorded state in the designated channel setting region based on a result of the key collation.

[0041] <3-3: Access of File> Access to a file in the present invention is performed, when giving a command for designating a specific channel to access a predetermined object file. For example, it is assumed that a process of reading data (e.g., customer number) for use in general bank business from a data file D11 under management of the file management region DF1 is performed in a state in which an application is defined as shown in FIG. 4. Here, it is more concretely assumed that an eighth record in the data file D11 is read. In the present invention, even in a case

where a specific file is accessed, a specific channel needs to be necessarily designated. Additionally, the channel to be designated has to be a channel in which a file management region for managing an access object file is being selected. In other words, it is surely necessary to select the file management region for managing the access object file beforehand using the specific channel, before giving the command to access the specific file.

[0042] In the above-described embodiment, the file management region DF1 is selected using the channel #1 by the selection command "SELECT #1 DF1" shown in FIG. 9①. Furthermore, the keys K3, K5 are brought into the unlocked state by the collation command shown in FIGS. 11①, ②. Then, it is possible to read the eighth record in the data file D11. Concretely, an access command "READ #1 D11 RFC8" shown in FIG. 11③ may be given. Upon receiving this command of the file access, the CPU 12 first judges whether or not an access object file (data file D11 in this example) belongs to the file management region (file management region DF1 in this example) specified by the identification information recorded in the recording portion (recording portion (2, 1) in this example) in the recorded state in the designated channel setting region. If the file does not belong, an error response indicating that access object file cannot be found is transmitted toward the reader/writer device 20. In the above-described example, since the access object file D11 is found as the

file belonging to the file management region DF1, any error is not generated.

[0043] If the file of the access object is found, subsequently it is judged whether or not access conditions are satisfied. That is, the CPU 12 compares the unlock information ("00101000" in this example) recorded in the recording portion (recording portion (2, 1) in this example) of the lowermost layer in the recorded state in the designated channel setting region with access conditions (e.g., access condition table shown in FIG. 5) set with respect to the access object file to judge whether or not the access conditions are satisfied. In this example, since the command "READ" is a read command belonging to command group 1. Therefore, according to the access condition table of FIG. 5, when the keys K3 and K5 are in an unlocked state, the access is possible. The unlock information of the recording portion (2, 1) shown in FIG. 11 satisfies the condition. Therefore, the access with respect to the data file D11 is permitted, and the contents of the eighth record are read toward the reader/writer device 20.

[0044] <3-4: File Management Region Selection No. 2> In a state shown in FIG. 11, the file management region DF1 is in a selected state using the channel #1. Therefore, in an access command which has designated the channel #1, the only file under the management of the file management region DF1 can be accessed. For example, it is here

assumed that to perform a process concerning foreign exchange, a necessity of accessing data file D121 under the management of the file management region DF1-2 occurs. In this case, the file management region DF1-2 needs to be re-selected anew. Then, it is assumed that the selection command "SELECT #1 DF1-2" is given as shown in FIG. 12①. Then, the state of the channel setting region is as shown in FIG. 12. FIG. 12 is different from FIG. 11 in that the recording portion (3, 1) is newly brought into a recorded state. Here it should be noted that the unlocked state of the recording portion (2, 1) in FIG. 11 is maintained as such in FIG. 12.

[0045] This respect to be noted becomes clearer, when FIG. 12 is compared with FIG. 10. FIG. 10 shows a state in which selection command "SELECT #1 DF1-2" is given in an initial state shown in FIG. 8, whereas FIG. 12 shows a state in which the same selection command "SELECT #1 DF1" is given in an interim state shown in FIG. 11. In other words, the state shown in FIG. 10 is a state obtained in a case where a path on a class from an initial state in which there is not anything to the file management region DF1-2 is defined. On the other hand, it can be said that the state shown in FIG. 12 is a state obtained in a case where the path on the class reaching the file management region DF1 is further extended to the file management region DF1-2 of class 3. In a case where the path is extended in this case, as to the unlocked state with respect to an extended

portion, "00000000" indicating non-unlocking is set, but the original unlocked state of the original portion is maintained as such.

[0046] In brief, in a case where the selection command to select the file management region using the predetermined channel is executed, the unlock information is maintained as such with respect to the recording portion (recording portions (1, 1) and (2, 1) in the example of FIG. 12) in which the identification information is not updated. A process to write the unlock information "00000000" indicating the non-unlocking is executed with respect to the recording portion (recording portion (3, 1) in the example of FIG. 12) in which the identification information is updated.

[0047] <3-5: Reference to Unlock Information of Upper Class> Additionally, since the file management region DF1-2 is selected using the channel #1 in the state shown in FIG. 12, the key collation process is performed with respect to the file management region DF1-2. When a necessary unlocking operation is performed, an access to the data file D121 under the management of the file management region DF1-2 is permitted. For example, it is assumed that the unlocking of three keys K3, K5, K6 has been required as the access conditions for reading the data from the data file D121. In this case, key collation commands "VERIFY #1 K3 ????" of FIG. 13①, "VERIFY #1 K5 ????" of FIG. 13②, and "VERIFY #1 K6 ????" of FIG. 13③

are given, and the unlocking operation is performed. Then, the channel setting region is brought into a state shown in FIG. 13, and it is recorded that the three keys K3, K5, K6 are brought into the unlocked states. Then, further, when an access command "READ #1D121 REC5" of FIG. 13④ is given, the access conditions are satisfied. Therefore, a fifth record is read on a reader/writer device 20 side.

[0048] However, since the collation of the keys K3, K5 has already completed in FIGS. 11①, ②, the collation process of the keys K3, K5 in FIG. 13①, ② is a redundant process operation. Practically, there are not a few cases in which the same key collation between the classes is set to the access conditions in this manner. For example, as shown in FIG. 4, the collation of a bank customer authentication key K3 with a bank branch authentication key K5 is set as the access condition in the file management region DF1 which manages the general bank business. In the file management region DF1-2 of the lower class, in addition to the key collation, further the collation of a foreign exchange handling authority key K6 is set as an additional access condition. This is a practically often used use mode. In this case, if the collation of the keys K3, K5 has been already completed at an access time of the file management region DF1, it is sufficient to only collate the key K6 when subsequently accessing the file management region DF1-2. A reference bit R shown in the access condition table of FIG. 5 is disposed considering this convenience.

[0049] For example, when the reference bit R of the access condition table for executing a read command with respect to the data file D121 is set to bit "1" (refer), instead of FIGS. 13① to ④, two commands of FIG. 14①, ② are only given. Then, the fifth record of the data file D121 is read on the reader/writer device 20 side. In this case, the key collation in a state in which the file management region DF1-2 is performed only with respect to the key K6. With regard to the unlock information of the recording portion (3, 1), the bit of the key K6 only is "1" (unlocked state) as shown in FIG. 14. However, since the unlock information of the upper class (unlock information of the recording portion (2, 1) in this example) is referred to, the unlock information of the file management region DF1-2 is handled as fused unlock information "00101100" (the fused unlock information is obtained by taking a logical sum of individual unlock information every bit in this example) in which unlock information "00101000" of the file management region DF1 of the upper class is fused with self unlock information "00000100". Accordingly, it is judged that the access conditions are satisfied.

[0050] When the setting capable of referring to the unlock information of the upper class is performed in this manner, any redundant collation process can be omitted, and sufficient security is secured while easy access is possible. Needless to say, with respect to a file requiring sophisticated security, the reference bit R is

set to "0", and the setting may be achieved in such a manner that the referring is not performed.